



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/360,068	07/23/1999	KEVIN J. PAGE	2322-0482	3638
27111	7590	02/09/2006		
GORDON & REES LLP 101 WEST BROADWAY SUITE 1600 SAN DIEGO, CA 92101			EXAMINER KLIMACH, PAULA W	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 02/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/360,068	Applicant(s) PAGE ET AL.	
	Examiner Paula W. Klimach	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 November 2005.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1, 2, 4-18, 20-27 and 29-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-2, 4-18, 20-27, and 29-35 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 11/14/05. The applicant amended claims 18 and 21-22, and 25 and cancelled claims 19 and 28. The presently pending claims are 1-2, and 4-18, 20-27, 29-35.

Response to Arguments

The applicants arguments filed 11/14/05 have been considered.

The applicant argued that Zuk teaches away from a combination of Zuk and Hohle. Whereas Zuk discloses the difficulty of rendering permanent hardware and software implementations of public key algorithms, Zuk does not completely teach away from the encryption in the smart card and therefore the security as recited in the claim language. Instead Zuk teaches the use of other algorithms for encryption on the smart card (column 3 lines 48-60). The algorithm is a variation of RSA that improves the performance and therefore is more suited for the smart card. As a result does not teach away from encryption in the smart card instead Zuk aims to improve the performance of the encryption algorithms used by smart cards.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

²⁷
~~28~~

Claims 18, 20, and 22-~~28~~ are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy et al. (6,226,744 B1) in view of Hilton et al (6,304,223) and further in view of Zuk (5,745,571)

In reference to claim 18, Murphy discloses exchanging the secure data through a communication network with the central computer system (column 4 lines 44-48 column 3 lines 30-50) wherein central computer system is the combination of computers as in Fig 1 parts 18, 22, 24, 20, and 26; and performing a security function on the data at the central computer system (column 6 lines 32-49). The system of Murphy discloses performing a security function at the smart card on secure data received from the central computer system (column 6 lines 56-63). Murphy further discloses the system having the ability to access restricted information from the servers. However the user uses the smart card for authentication in order to receive the data. Access control using the smart card is a security function that is performed on the secure data, restricted data, in order for the user to receive the restricted data.

Although Murphy discloses a smart card that is coupled with a client device (Fig. 1), the smart card is not a contactless smart card.

Hilton discloses a contactless card smart card (abstract). Secure data is exchanged through a radio frequency communication channel with the smart card (column 3 lines 50-67).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the card reader and smart card in Murphy to be contactless RF communications as in Hilton. One of ordinary skill in the art would have been motivated to do this because the device will not require contact between the smart card and the validator (Hilton column 1 lines 10-15).

In reference to claim 20, since the data is transported over the network as shown in Fig 1, the data is evidently formatted in accordance with the communication network protocol for the network in Fig. 1, and reformatted at the central computer. The data is transmitted through the communication network as shown in Fig. 1.

In reference to claim 22, the secure data is exchanged over a baseband channel, Murphy fig 1 where the smart card reader is connected to a client terminal, which then connects to the network. Murphy discloses a system that exchanges data with a central computer.

In reference to claim 25, the smart card reader described by Murphy is connected to a client terminal, Fig. 1. The smart card reader described by Hilton is a proximity card. In Murphey Fig. 1 the access points are connected to a network. The central computer authenticates the smart card; therefore has a security device coupled to it (column 6 lines 32-49).

In reference to claim 26, the client terminal in Murphy works on the Internet (Fig. 1).

In reference to claims 23, the secure data is not deciphered within the communication link (Fig. 1).

In reference to claims 24, the step of subjecting the secure data to a security function only at the smart card and at the and at the central computer (column 5 lines 51-67).

In reference to claim 27 is the same discussion as in the reference to claim 23 and 24.

Claims 1, 2, 4-17, 29-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Hohle et al (6,101,477) in view of Zuk (5,745,571) and further in view of Hilton.

In reference to claims 1 and 29, Hohle teaches a system for establishing a secure connection between a smart card and a central computer (issuer 10), Fig.10. The system uses the

Art Unit: 2135

method of outgoing secure signal transmitted from the smart card to produce an out going secure data signal, column 3 lines 31-51. The connection described by Hohle is a secure connection because the system uses the DES algorithm for encryption of a random number in the challenge/response authentication, column 11 line 63 to column 12 line 36. Since that data is sent over the network disclosed in Fig. 10, it must be formatted in accordance with a communication network protocol to produce an outgoing format. Finally, in column 5 line 64 to column 6 line 4, the formatted signal is sent to the central computer system, issuer 10. The card is described as communicating with the issuer 10 through the client host (the access point) and therefore, for communication to take place a signal must be sent from the card to the central computer system.

Although Hohle discloses a system wherein the smart card transactions have a security dimension (column 21 line 43 to column 22 line 36), Hohle does not expressly disclose the outgoing transmission sent without deciphering the data.

Zuk discloses encrypting secret data in the smart card and therefore transmitting the data from the smart card reader to the central station without deciphering the information (column 5 lines 62-67).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the data in the smart card as in Zuk in the system of Hohle. One of ordinary skill in the art would have been motivated to do this because it would discourage a third party from intercepting unencrypted data (Zuk column 1 lines 1-67).

Although Hohle discloses secure contactless communications that utilize inductive couplings, Hohle does not disclose RF communications and therefore demodulating an outgoing radio frequency signal transmitted from the smart card to produce an outgoing signal.

Hilton discloses RF communications between a smartcard and the field device (Fig. 4). Therefore Hilton suggests the demodulation of an outgoing radio frequency signal transmitted from the smart card to produce an outgoing signal (column 3 line 50 to column 4 line 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the RF communication as in the system of Hilton between the smart card and central system of Hohle. One of ordinary skill in the art would have been motivated to do this because RF communication and inductive communication links are interchangeable methods of contactless communication for smart cards (column 1 lines 11-20).

In reference to claims 2 and 30, Hohle subjects the out going data to a security function only in the smart card and the central computer system. The data is “signed” by the central computer by producing the MAC, column 22 lines 53-58. The card then produces a MAC based on the received message and compares them and the two MACs will not match if the message or the wrong key has been used, column 22 lines 59-67.

In reference to claim 4, the data at the central computer (the bank computer 150) is transformed back into plain text, column 16 lines 45-47. The data is sent over the network to the central computer, column 16 line 34, as a result, it is apparent that it must have been reformatted.

In reference to claim 5, the system disclosed by Hohle receives the incoming secure formatted signal from the central computer as discussed in claim 1. Wilson teaches that

communication in the opposite direction, in this case from the central computer to the smart card, may be performed in the same way, column 15 lines 30-43.

In reference to claims 6 and 33, the Hohle reference teaches of contactless cards using phase, frequency and amplitude modulation, column 3 lines 44-45, therefore the reader demodulates the signal sent over radio frequencies. Wilson teaches applying cipher text to a decryption module to arrive at the plain text, column 15 lines 30-51.

In reference to claim 7, the security function is as discussed above in the discussion for claim 6.

In reference to claims 8 and 34, the data is encoded in the smart card, as discussed for claim 3, which would make the outgoing data signal secure.

In reference to claim 9, Hohle further teaches generating a MAC at the smart card and then appending it to the outgoing data as a electronic seal to sign the data, column 22 lines 47-67.

In reference to claim 10, 11, 15, 16, and 35, Hohle discusses the use of a MAC to seal messages with in order to detect an unauthorized modification of the outgoing data, column 22 lines 47-67.

In reference to claim 14, Hohle discloses a system where a MAC and appended to the message, column 22 lines 47-67.

In reference to claim 17, encoding using a smart card and transmitting the radio frequencies, the modulation of the outgoing radio frequency, formatting of the secure data, and the transmission of outgoing data has been discussed in reference to claim 1. The reformatting of the outgoing secure signal and decoding of the signal has been discussed in reference to claim 4. While the reference to claim 8 discusses the encoding of information from the central

Art Unit: 2135

computer. It is evident that since the signal is sent over the network, it would be formatted to produce an incoming formatted signal. The reference to claim 5 discusses the receiving, reformatting, and transmission of the secure signal. Finally the demodulation and the decoding of the secure data signal is discussed in reference to claim 6.

In reference to claim 12-13, 31-32, Zuk discusses the use of a smart card to encrypt data using software stored on the card and being able to perform the communication in both directions (column 5 lines 49-67).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the data in the smart card as in Zuk in the system of Hohle. One of ordinary skill in the art would have been motivated to do this because it would discourage a third party from intercepting unencrypted data (Zuk column 1 lines 1-67).

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hohle in view of Murphy et al (6, 226, 744 B1) and further in view of Hilton.

In reference to claim 21, Hohle discloses a system for communication between a smart card and a central computer with the ability for some of the software to exist outside the card and be downloaded during transaction, column 4 lines 49-54. The secure data is exchanged with the smart card reader, column 3 lines 42-45. Although Hohle discloses a system that includes an authentication process, Hohle does not disclose a system where interface software can be downloaded to perform the authentication.

Murphy discloses a system where a user can download a smart card interface module to the client terminal for the authentication process, column 6 lines 8-25. The secure gateway

Art Unit: 2135

server corresponds to the HTTP server recited in claim 21. A HTTP server by definition is a software that uses HTTP documents and any associated files and scripts when requested by a client, such as a web browser. The gateway server disclosed by Murphy communicates with the client (web browser) and therefore by necessity uses HTTP to communicate (column 6 lines 8-21).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the Client terminal 14 described by Murphy to download the interface for the authentication process disclosed by Hohle and using the smart card and smart card reader disclosed by Hohle. One of ordinary skill in the art would have been motivated to do this because users would be able to access restricted information with the smart card without having to install software, column 3 lines 24-28.

Although Hohle discloses secure contactless communications that utilize inductive couplings, Hohle does not disclose RF communications and therefore demodulating an outgoing radio frequency signal transmitted from the smart card to produce an outgoing signal.

Hilton discloses RF communications between a smartcard and the field device (Fig. 4). Therefore Hilton suggests the demodulation of an outgoing radio frequency signal transmitted from the smart card to produce an outgoing signal (column 3 line 50 to column 4 line 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the RF communication as in the system of Hilton between the smart card and central system of Hohle. One of ordinary skill in the art would have been motivated to do this because RF communication and inductive communication links are interchangeable methods of contactless communication for smart cards (column 1 lines 11-20).

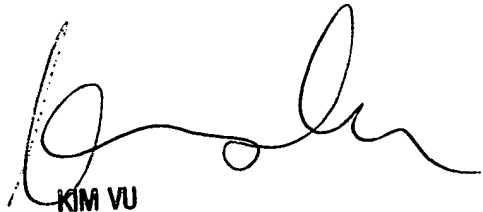
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2101